https://doi.org/10.69639/arandu.v13i2.2165

Responsabilidad penal por criminalidad organizada en entornos digitales

Criminal liability for organized crime in digital environments

Katty Karina Rodríguez Pilco
kattyrodriguez@uti.edu.ec
https://orcid.org/0009-0002-7154-8172
Universidad de Chimborazo
Ecuador – Chimborazo

Luis Andrés Chimborazo Castillo
luischimborazo@uti.edu.ec
https://orcid.org/0000-0003-1850-4074
Universidad de Chimborazo
Ecuador - Chimborazo

Artículo recibido:18 marzo 2026- Aceptado para publicación:20 abril 2026
Conflictos de intereses: Ninguno que declarar.

RESUMEN

La criminalidad organizada ha experimentado una transformación profunda como consecuencia del desarrollo tecnológico y la expansión de los entornos digitales. Las organizaciones criminales han dejado de operar únicamente en espacios físicos para consolidarse en el ciberespacio, utilizando plataformas digitales, sistemas automatizados e inteligencia artificial para ejecutar delitos complejos como el lavado de activos, la trata de personas, la extorsión y otras formas de macro criminalidad transnacional. Esta evolución ha incrementado su capacidad operativa, su alcance geográfico y la dificultad para identificar y sancionar a los responsables. En el contexto ecuatoriano, si bien el ordenamiento jurídico ha incorporado disposiciones relacionadas con delitos informáticos y criminalidad organizada, persisten importantes limitaciones normativas, técnicas y operativas. Entre las principales problemáticas se identifican la insuficiente regulación específica para conductas digitales complejas, las dificultades en el manejo y valoración de la evidencia digital, la escasez de operadores de justicia especializados y la falta de protocolos claros frente al uso de tecnologías emergentes como la inteligencia artificial. Estas debilidades generan obstáculos para la atribución efectiva de responsabilidad penal y favorecen escenarios de impunidad. El estudio, de enfoque cualitativo y documental, analiza críticamente el marco normativo vigente, las capacidades institucionales del sistema penal y los desafíos que plantea la tecnología en la persecución del delito organizado digital. A partir del análisis doctrinal, normativo y comparado, se evidencia la necesidad de fortalecer el sistema penal ecuatoriano mediante reformas legales, capacitación especializada, mejora de los mecanismos probatorios y

cooperación internacional, garantizando siempre el respeto a los derechos fundamentales y a los principios del debido proceso.

Palabras clave: responsabilidad penal, criminalidad organizada, entornos digitales, delitos tecnológicos, prueba digital

ABSTRACT

Organized crime has undergone a profound transformation as a result of technological development and the expansion of digital environments. Criminal organizations no longer operate exclusively in physical spaces but have consolidated their activities in cyberspace, using digital platforms, automated systems, and artificial intelligence to carry out complex crimes such as money laundering, human trafficking, extortion, and other forms of transnational macro-criminality. This evolution has increased their operational capacity, geographical reach, and the difficulty of identifying and prosecuting those responsible. In the Ecuadorian context, although the legal system has incorporated provisions related to cybercrime and organized crime, significant normative, technical, and operational limitations persist. Among the main challenges are insufficient regulation of complex digital conduct, difficulties in the handling and assessment of digital evidence, a shortage of specialized justice operators, and the lack of clear protocols for the use of emerging technologies such as artificial intelligence. These shortcomings hinder the effective attribution of criminal responsibility and foster scenarios of impunity. This qualitative and documentary study critically examines the current legal framework, the institutional capacities of the criminal justice system, and the challenges posed by technology in the prosecution of organized digital crime. Based on doctrinal, normative, and comparative analysis, the study highlights the need to strengthen Ecuador's criminal justice system through legal reforms, specialized training, improved evidentiary mechanisms, and international cooperation, while always ensuring respect for fundamental rights and due process principles.

Keywords: criminal liability, organized crime, digital environments, technological crimes, digital evidence

INTRODUCCIÓN

La rápida expansión de las tecnologías digitales ha alterado de manera profunda las dinámicas de la criminalidad organizada actual, los grupos delictivos que antes se organizaban en jerarquías territoriales, han cambiado hacia estructuras transnacionales en red que operan en espacios virtuales con altos niveles de anonimato, funcionalidad descentralizada y gran sofisticación técnica, este cambio ha dado lugar a modalidades complejas de criminalidad digital a gran escala, donde se utilizan plataformas tecnológicas para cometer delitos como el lavado de dinero a través de criptoactivos, la trata de personas facilitada por redes sociales, la extorsión informática, el sicariato coordinado a distancia y la implementación de inteligencia artificial para la automatización y encubrimiento de actividades delictivas.

Este fenómeno no solo altera las formas de llevar a cabo los delitos, sino que también pone a prueba las categorías tradicionales del derecho penal, especialmente en lo que respecta a la imputación, autoría, participación y la asignación de responsabilidad dentro de sistemas organizados digitalizados, en escenarios regionales como el de Ecuador, donde se ha evidenciado el crecimiento de organizaciones criminales transnacionales con capacidades tecnológicas en aumento, la criminalidad organizada en el ámbito digital representa un desafío estructural para el sistema de justicia penal y para el mantenimiento efectivo del Estado de derecho.

Ante esta situación, surge una cuestión legal fundamental: ¿tiene el sistema penal ecuatoriano un marco regulatorio, técnico e institucional adecuado para atribuir responsabilidad penal por delitos organizados en entornos digitales, al mismo tiempo que se asegura el respeto a los principios de legalidad, proporcionalidad y debido proceso?

El asunto va más allá de simplemente definir delitos informáticos, como señala Ferrajoli (2011), la legitimidad del poder punitivo en un Estado de derecho está estrechamente vinculada al respeto de las garantías fundamentales y al principio de legalidad, En el entorno digital, el aumento del derecho penal puede acarrear riesgos de sobrecriminalización y vigilancia excesiva, sobre todo cuando se utilizan técnicas especiales de investigación como interceptaciones, infiltraciones virtuales y monitoreo masivo de datos sin controles judiciales rigurosos.

En línea con esta perspectiva crítica, Zaffaroni (2015) argumenta que la respuesta legislativa a nuevos tipos de delitos tiende a ser una expansión punitiva simbólica que incrementa las penas sin resolver los déficits en la investigación, esta tendencia es especialmente significativa en el contexto ecuatoriano, donde el Código Orgánico Integral Penal incluye figuras relacionadas con el crimen organizado y los delitos informáticos, pero enfrenta dificultades prácticas en la obtención, conservación y evaluación de pruebas digitales.

A partir de la teoría del dominio del hecho, Roxin (2014) aporta herramientas conceptuales clave para examinar la responsabilidad penal dentro de estructuras organizadas complejas, sin embargo, al aplicar estas categorías a organizaciones criminales que operan

digitalmente suscita preguntas sobre la atribución de autoría mediata en redes descentralizadas, el uso de intermediarios tecnológicos y la posible responsabilidad derivada del uso de sistemas automatizados o inteligencia artificial.

El trabajo de investigación se centra en el estudio de la responsabilidad penal asociada a la criminalidad organizada en el ámbito digital en Ecuador, se examinan tres áreas interconectadas: (I) la adecuación y consistencia del sistema legal penal actual ante las nuevas manifestaciones de macrocriminalidad en línea; (II) las capacidades tanto técnicas como institucionales para llevar a cabo investigaciones y manipular pruebas digitales; y (III) los retos teóricos que surgen al intentar asignar responsabilidad tanto a nivel individual como colectivo en organizaciones criminales mediadas por la tecnología.

La hipótesis que guía esta investigación postula que, aunque el sistema penal de Ecuador ha implementado herramientas legales para abordar la criminalidad organizada en el entorno digital, todavía existen deficiencias técnicas, de interpretación y estructurales que impiden una asignación de responsabilidad penal que sea efectiva y que respete los derechos fundamentales. Esto crea conflictos entre la eficacia de las penas y la protección de los derechos.

Marco Teórico

Criminalidad organizada en entornos digitales: evolución reciente y fundamentos conceptuales

La criminalidad organizada actual ha sufrido un cambio estructural debido al avance de la digitalización en las actividades económicas y sociales, a diferencia de los grupos criminales clásicos, que se distinguían por tener jerarquías rígidas y áreas de acción bien definidas, las redes delictivas contemporáneas funcionan con modelos descentralizados, operan a nivel internacional y utilizan tecnología avanzada (UNODC, 2023). Este fenómeno se ha denominado "crimen organizado digital", que se refiere a la interacción entre estructuras criminales ya establecidas y la utilización estratégica de la tecnología de la información.

De acuerdo con el Informe Global sobre el Crimen Organizado 2023 de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, 2023), las organizaciones delictivas han integrado herramientas digitales para ampliar mercados ilegales, mejorar el proceso de lavado de dinero mediante criptomonedas y complicar la identificación de flujos financieros, este avance ha provocado una transformación en la naturaleza del crimen organizado, donde el ciberespacio se presenta no solo como un medio, sino como un entorno operativo fundamental.

Leukfeldt, Lavorgna y Kleemans (2020), en una investigación publicada en Trends in Organized Crime, afirman que las organizaciones criminales están implementando modelos híbridos, que combinan actividades tradicionales con avanzadas capacidades digitales, este rasgo híbrido indica que el análisis de la criminalidad organizada no puede realizarse solo desde enfoques convencionales, sino que es necesario integrar visiones criminológicas y tecnológicas.

En consonancia con esto, Broadhurst et al. (2021) señalan que el uso de plataformas digitales y mercados en la dark web ha disminuido las barreras de acceso a actividades ilegales, facilitando la cooperación internacional entre individuos que no necesariamente se conocen en persona, esta situación desafía las definiciones tradicionales de estructura organizada que se establecen en documentos como la Convención de Palermo.

Responsabilidad penal e imputación en estructuras criminales digitalizadas

Desde la teoría penal actual, uno de los grandes retos se centra en la asignación de culpa en organizaciones criminales descentralizadas, según Bock (2021), el delito organizado en el ámbito digital exige una nueva interpretación de las nociones de autoría y participación, sobre todo cuando los delitos se llevan a cabo a través de la intermediación tecnológica o de una automatización parcial.

La operatividad descentralizada, el anonimato en la web y el uso de criptografía complican la tarea de identificar quién tiene el control efectivo sobre el acto delictivo, En este marco, es necesario ajustar la teoría del dominio del hecho a situaciones en las que el control sobre la cadena de causas se puede ejercer de manera remota, utilizando programación informática o supervisión algorítmica.

El incremento en el uso de inteligencia artificial para llevar a cabo actividades ilegales genera preguntas sobre la previsibilidad de los resultados y la creación de riesgos que no están permitidos por la ley Hildebrandt (2020) que argumenta que los sistemas automatizados no eximen a las personas de responsabilidad, pero hacen que el enfoque se dirija hacia aquellos que diseñan, supervisan o utilizan la tecnología con propósitos ilícitos.

Criminalidad organizada digital en América Latina

En la región de América Latina, la adopción de herramientas digitales ha potenciado las redes criminales existentes, especialmente en actividades vinculadas al narcotráfico, la trata de personas y el blanqueo de capitales, el informe de Europol sobre Amenazas del Crimen Organizado y Grave (2021) señala que el empleo de criptomonedas y plataformas de mensajería segura ha reforzado la capacidad de estas organizaciones para evadir el control judicial.

Estudios recientes indican que, en el área andina, el uso de tecnologías digitales ha facilitado la coordinación de actividades logísticas, el reclutamiento de individuos y el financiamiento ilegal (InSight Crime, 2022), esto significa que los gobiernos deben actualizar no solo sus leyes, sino también mejorar sus habilidades técnicas en investigación y análisis forense digital.

Criminalidad organizada

La criminalidad organizada constituye un fenómeno de alcance internacional que ha sido abordado desde diversas perspectivas teóricas dentro de la criminología y el derecho penal, uno de los enfoques explicativos más influyentes es la teoría de la elección racional, la cual sostiene que los individuos que integran organizaciones criminales actúan con base en un cálculo

estratégico de costos y beneficios, orientado a maximizar ganancias y minimizar riesgos, desde esta óptica, el crimen organizado no responde a impulsos irracionales o espontáneos, sino a decisiones planificadas que se insertan en estructuras estables de cooperación ilícita.

Complementariamente, la teoría de la anomia explica el surgimiento y expansión de estas organizaciones como consecuencia del debilitamiento de los marcos normativos y de la erosión de la legitimidad institucional. En contextos donde las oportunidades legales de movilidad social son limitadas y las instituciones estatales carecen de credibilidad, las organizaciones criminales encuentran condiciones propicias para consolidarse y ofrecer mecanismos alternativos de acceso a recursos y poder.

No obstante, el concepto de "criminalidad organizada" ha sido objeto de críticas por su amplitud y ambigüedad semántica. Su uso indiscriminado puede diluir las diferencias entre delincuencia común, estructuras empresariales ilícitas y redes transnacionales complejas. Por ello, resulta indispensable delimitar conceptualmente el fenómeno a partir de criterios como estabilidad estructural, división funcional de roles, finalidad lucrativa y capacidad de infiltración institucional.

La dimensión geopolítica del crimen organizado

En América Latina, el crimen organizado transnacional ha superado la esfera tradicional de la seguridad ciudadana para configurarse como un desafío geopolítico estructural, esta transformación responde a la capacidad de las organizaciones delictivas para expandirse más allá de las fronteras nacionales, aprovechando debilidades institucionales, corrupción sistémica y vacíos normativos.

Como señala Lagos Flores (2024), estas estructuras no solo disputan el control territorial, sino que inciden directamente en la dinámica política local, estableciendo redes de cooperación que involucran actores ilegales y, en ocasiones, sectores estatales y privados, el crimen organizado deja de ser un problema meramente policial para convertirse en un factor de desestabilización democrática.

Ejemplos paradigmáticos de esta expansión son el Primer Comando de la Capital (PCC) en Brasil, el denominado "Tren de Aragua" de origen venezolano y las disidencias de las FARC en la región andina. Estas organizaciones operan en zonas fronterizas estratégicas, suplantando funciones estatales, imponiendo reglas propias y generando legitimidades paralelas que erosionan la soberanía y la gobernabilidad.

La consecuencia jurídica de este fenómeno es clara: el derecho penal nacional resulta insuficiente cuando las estructuras delictivas operan mediante redes transnacionales, financiamiento ilícito globalizado y articulación con mercados internacionales.

Desde una perspectiva epistemológica, comprender el crimen organizado exige superar las representaciones mediáticas simplificadoras. Paulo Freire (2008), al sostener que "la lectura del mundo precede a la lectura de la palabra", invita a analizar críticamente los discursos que

configuran nuestra percepción del fenómeno. Esta advertencia resulta pertinente, pues la narrativa mediática suele romantizar o distorsionar la realidad estructural de la macrocriminalidad.

En el plano criminológico, la noción de crimen organizado atraviesa una crisis definitoria producto de la mutación constante de los mercados ilícitos, de la Corte Ibáñez y Giménez-Salinas Framis, citados por Sampó (2017), sostienen que estas organizaciones no solo persiguen lucro ilícito, sino que aseguran su permanencia mediante violencia sistemática, corrupción e infiltración en la economía formal.

Olaeta y Comba (2016) profundizan esta idea al describir la convergencia entre redes empresariales y estructuras criminales, donde actores públicos y privados pueden confluir en esquemas de maximización de beneficios ilícitos, este entrelazamiento evidencia que el crimen organizado no se ubica al margen del sistema económico, sino que interactúa con él, penetrándolo y distorsionándolo.

Freire (2023) subraya que, pese al reconocimiento internacional del vínculo entre corrupción y criminalidad organizada, los mecanismos de prevención ética en el sector público continúan siendo insuficientes, resulta particularmente llamativo que ciertas corporaciones privadas hayan implementado estándares de prevención más estrictos que algunos marcos regulatorios estatales, lo que revela una asimetría preocupante en materia de control institucional.

Evolución de la criminalidad organizada en Perú y Ecuador: la trata de personas como una manifestación estructural

En el contexto de Perú, las agrupaciones criminales se establecen como entidades jerárquicas, estables y con funciones diferenciadas, enfocándose en el lucro ilícito de manera sostenida, Reyes Valdivia (2025) señala que la permanencia estructural es un rasgo característico que las diferencia de la delincuencia común, resaltando la existencia de roles claramente definidos, distribución de tareas y coordinación sistemática, esta estabilidad permite una especialización interna y una expansión en el territorio, factores que aumentan su eficacia operativa.

Cabrera (2025) menciona que estas redes buscan no solo beneficios económicos, sino que también utilizan la violencia y la corrupción como herramientas esenciales para garantizar su continuidad y protección institucional, la corrupción, en específico, actúa como un acelerador que facilita el tráfico de víctimas, la falsificación de documentos y la evasión de los controles estatales.

Una de las manifestaciones más alarmantes de esta estructura delictiva en Perú es la trata de personas, este crimen ha mostrado un aumento continuo en áreas de minería ilegal, explotación sexual y trabajo forzado, a pesar de que el marco internacional se basa en el Protocolo de Palermo (2000), su aplicación en el ámbito judicial enfrenta retos significativos, Montoya (2016) señala que uno de los principales problemas interpretativos surge de la evaluación del consentimiento de las víctimas, en situaciones de vulnerabilidad socioeconómica, desigualdad estructural o dependencia económica, el consentimiento aparente carece de validez jurídica, por lo que el

enfoque debe concentrarse en los métodos delictivos —engaño, coacción, abuso de poder o situaciones de vulnerabilidad y no en la apariencia de libre elección.

En Ecuador, el fenómeno presenta similitudes estructurales con el de Perú, aunque ha intensificado su manifestación en los últimos años debido al fortalecimiento de grupos criminales con vínculos transnacionales, la trata de personas se ha relacionado con dinámicas de migración irregular, explotación sexual, trabajo forzado y reclutamiento a través de redes sociales y plataformas digitales.

A diferencia de los métodos tradicionales de captación, en la actualidad se observa un uso estratégico de entornos digitales para el reclutamiento, traslado y control de las víctimas. Las organizaciones utilizan redes sociales, aplicaciones de mensajería cifrada y anuncios de empleos falsos como medios de captación, este componente tecnológico agrega una dimensión nueva al fenómeno, ya que complica la obtención de pruebas y amplía el alcance territorial de las redes.

El marco legal ecuatoriano tipifica la trata de personas dentro del Código Orgánico Integral Penal, alineándose formalmente con los estándares del Protocolo de Palermo. Sin embargo, en la práctica, la investigación enfrenta limitaciones técnicas relacionadas con la recolección de evidencia digital, la cooperación internacional y la identificación de estructuras jerárquicas en redes descentralizadas.

Criminalidad del poder y derecho penal mínimo

Ferrajoli (2006) introduce la categoría de "criminalidad del poder" para describir conductas ilícitas protagonizadas por élites políticas, económicas o estructuras jerarquizadas con capacidad de influencia sistémica. Este fenómeno representa una amenaza estructural para el Estado de derecho, pues compromete derechos fundamentales y estabilidad democrática.

- El autor distingue tres dimensiones:
- Poderes criminales tradicionales (mafias, terrorismo internacional).
- Grandes poderes económicos transnacionales que operan en zonas de débil regulación.
- Poderes públicos criminales, donde agentes estatales participan en tramas de corrupción o violaciones graves.

Frente a esta realidad, Ferrajoli propone un modelo de derecho penal mínimo, sustentado en el principio de ultima ratio, en la limitación de la intervención penal a las ofensas más graves y en la eliminación de la selectividad estructural del sistema.

El debate sobre el bien jurídico protegido en el delito de lavado de activos no es pacífico. Caraballo (2020) sistematiza tres corrientes doctrinales:

- Salud pública (cuando el delito precedente es narcotráfico).
- Administración de justicia (como forma de encubrimiento agravado).
- Orden socioeconómico (tesis predominante).

La última postura sostiene que la inyección de capitales ilícitos distorsiona la competencia, desestabiliza mercados y erosiona la transparencia económica. Desde esta perspectiva, la política criminal no solo busca recuperar activos, sino preservar la integridad del sistema financiero.

Conceptualización del terrorismo en el Código Orgánico Integral Penal ecuatoriano

A diferencia del modelo español, que adopta una estructura binaria explícita en el artículo 573 del Código Penal (delito grave + finalidad terrorista específica), el ordenamiento jurídico ecuatoriano regula el terrorismo dentro del Código Orgánico Integral Penal (COIP) bajo una configuración que combina elementos objetivos y subjetivos, pero sin estructurar formalmente el tipo en términos binarios.

El COIP tipifica el terrorismo estableciendo como elemento central la ejecución de actos que, por su naturaleza y gravedad, tengan como finalidad causar terror en la población, obligar a una autoridad pública a realizar o abstenerse de realizar un acto, o desestabilizar el orden constitucional o la seguridad del Estado, en este sentido, la estructura típica ecuatoriana también integra dos componentes esenciales:

La comisión de conductas objetivamente graves (violencia contra personas, bienes estratégicos o infraestructura crítica).

La concurrencia de una finalidad específica de intimidación colectiva o desestabilización institucional.

Desde una perspectiva dogmática, esta configuración responde igualmente a una lógica binaria material, aunque no formulada de manera tan sistemática como en el derecho español.

El elemento subjetivo especial la finalidad de causar terror o alterar el orden constitucional constituye el núcleo diferenciador respecto de otros delitos comunes, sin embargo, esta exigencia plantea problemas interpretativos similares a los señalados en la doctrina española respecto al concepto de “paz pública”.

En el Ecuador, nociones como “seguridad del Estado” o “orden público” pueden presentar un margen de indeterminación si no se interpretan restrictivamente conforme a los principios de legalidad y taxatividad, en un Estado constitucional de derechos, el tipo penal de terrorismo debe aplicarse con criterios estrictos, evitando que conductas de protesta social, disturbios o manifestaciones violentas sean subsumidas indebidamente bajo esta categoría.

Aunque el COIP no establece una categoría autónoma denominada “terrorismo cibernético” de manera expresa como el artículo 573.2 del Código Penal español, el ordenamiento ecuatoriano permite que conductas realizadas mediante medios tecnológicos sean subsumidas dentro del tipo general de terrorismo cuando concurran los elementos objetivos y subjetivos exigidos.

Esto implica que ataques informáticos contra infraestructura crítica, sabotajes digitales a sistemas financieros, energéticos o gubernamentales, o la difusión coordinada de amenazas con

finalidad intimidatoria podrían configurar terrorismo si cumplen la exigencia de finalidad desestabilizadora o de generación de terror colectivo.

No obstante, doctrinalmente surge el debate acerca de si resulta necesaria una tipificación autónoma del terrorismo digital o si basta con integrar los medios tecnológicos como modalidades comisivas dentro del tipo general, desde una perspectiva sistemática, podría sostenerse que la creación de una categoría independiente generaría riesgos de sobreexpansión punitiva, especialmente cuando muchos delitos informáticos graves ya se encuentran tipificados en el propio COIP.

Esta convergencia plantea interrogantes relevantes:

¿Cuándo una organización criminal que genera terror sistemático debe calificarse como estructura terrorista?

¿Es suficiente la violencia reiterada o se requiere un propósito político específico?

¿Cómo se diferencia la delincuencia organizada altamente violenta del terrorismo en sentido estricto?

La respuesta exige una interpretación restrictiva, pues el terrorismo no puede convertirse en una categoría residual para sancionar cualquier forma de macrocriminalidad violenta, de lo contrario se vulneraría el principio de legalidad y se ampliaría desproporcionadamente el ius puniendi estatal.

RESULTADOS Y DISCUSIÓN

La criminalidad organizada en entornos digitales constituye uno de los mayores desafíos contemporáneos para los sistemas penales latinoamericanos, particularmente en contextos institucionales frágiles como el ecuatoriano, el análisis realizado evidencia que el problema no radica exclusivamente en la insuficiencia normativa, sino en la disociación estructural entre el desarrollo tecnológico de las organizaciones criminales y la capacidad operativa del Estado para investigarlas y sancionarlas de manera eficaz y garantista.

Entre 2020 y 2026, diversos informes internacionales como el Global Organized Crime Index (2021, 2023) y reportes recientes de UNODC (2022–2024) han señalado que las organizaciones criminales han incorporado de forma sistemática herramientas digitales para fortalecer su resiliencia operativa, esta transformación no solo amplía el radio de acción de las estructuras delictivas, sino que redefine las categorías tradicionales del derecho penal, obligando a reconsiderar los criterios clásicos de territorialidad, autoría y participación.

En el caso ecuatoriano, el Código Orgánico Integral Penal incorpora tipos penales vinculados a delincuencia organizada y delitos informáticos; sin embargo, la eficacia de estas disposiciones enfrenta obstáculos prácticos significativos, la evidencia empírica muestra que persisten limitaciones en materia de peritaje digital, cadena de custodia electrónica, análisis forense de dispositivos y cooperación internacional inmediata, la criminalidad organizada digital

opera mediante redes descentralizadas, plataformas cifradas y criptomonedas, lo que exige capacidades técnicas que superan el diseño tradicional de las fiscalías especializadas.

Esta brecha técnica no es exclusiva de Ecuador, estudios recientes en Perú, Argentina y Colombia (2021–2025) coinciden en que la persecución penal digital requiere una profesionalización sostenida de operadores judiciales y una infraestructura tecnológica robusta, el problema adquiere una dimensión particularmente crítica cuando se analiza desde la perspectiva garantista, como advierte Ferrajoli en su teoría del constitucionalismo penal, la expansión del derecho penal frente a nuevas amenazas no puede justificar la flexibilización de garantías fundamentales, la respuesta punitiva frente al crimen organizado digital debe mantenerse dentro de los límites de legalidad estricta, taxatividad y proporcionalidad.

Aquí emerge una tensión estructural mientras las organizaciones criminales se adaptan con rapidez a la innovación tecnológica, el Estado enfrenta la tentación de expandir el ius puniendi mediante figuras amplias, técnicas especiales de investigación invasivas y mecanismos de vigilancia digital que pueden comprometer derechos como la privacidad, la inviolabilidad de comunicaciones y el debido proceso, esta tensión ha sido advertida también por la doctrina latinoamericana reciente (2020–2024), que identifica el riesgo de un "populismo punitivo tecnológico" en contextos de crisis de seguridad.

Otro aspecto relevante es la transnacionalización del fenómeno, la digitalización permite que redes dedicadas al lavado de activos, trata de personas o extorsión operen simultáneamente en múltiples jurisdicciones sin presencia física estable, esto desafía el principio clásico de territorialidad penal y exige una cooperación internacional más ágil, si bien Ecuador ha suscrito instrumentos multilaterales como la Convención de Palermo, la implementación efectiva de mecanismos de asistencia judicial recíproca sigue siendo lenta y burocrática, lo que favorece la impunidad estructural.

La interacción entre criminalidad organizada y tecnología no solo incrementa la complejidad probatoria, sino que altera la estructura misma del delito, el uso de redes sociales para reclutamiento en trata de personas, la utilización de criptomonedas para lavado de activos y la coordinación logística mediante plataformas cifradas demuestran que el entorno digital ya no es un simple medio, sino un espacio estructural de operación criminal, esto obliga a repensar la imputación penal en términos funcionales y no meramente físicos.

Particularmente complejo resulta el debate sobre inteligencia artificial, entre 2020 y 2026, la literatura especializada ha subrayado que los sistemas algorítmicos pueden ser utilizados para automatizar fraudes, manipular información o facilitar ciberataques. Sin embargo, los sistemas de IA carecen de capacidad normativa y conciencia jurídica; por tanto, la responsabilidad penal no puede atribuirse a la máquina, sino a quienes diseñan, programan, supervisan o instrumentalizan estos sistemas con fines ilícitos.

El desafío dogmático consiste en determinar el grado de dominio del hecho cuando la ejecución material se produce mediante un sistema automatizado, la teoría del dominio funcional debe adaptarse a escenarios donde el control del riesgo se ejerce a través de programación algorítmica o decisiones de configuración tecnológica, la atribución de responsabilidad exige probar conocimiento, previsibilidad y control efectivo, elementos que pueden diluirse en estructuras organizadas complejas.

La criminalidad organizada digital no puede analizarse aisladamente de factores estructurales como corrupción institucional, desigualdad socioeconómica y debilidad del control administrativo, informes regionales recientes han evidenciado que las organizaciones criminales logran penetrar instituciones públicas mediante sobornos, facilitando acceso a información estratégica y protección frente a investigaciones, sin un fortalecimiento real de la integridad institucional, la reforma normativa resulta insuficiente.

Desde una perspectiva comparada, Perú ha avanzado en la creación de fiscalías especializadas en crimen organizado con unidades técnicas de análisis digital; Argentina ha implementado protocolos específicos para evidencia informática; y Colombia ha fortalecido la cooperación con agencias internacionales en materia de cibercrimen. Ecuador, aunque ha realizado avances normativos, aún enfrenta desafíos en la consolidación de unidades técnicas especializadas con autonomía operativa y recursos sostenidos.

El estudio confirma que la eficacia del sistema penal frente a la criminalidad organizada digital depende de cinco factores estructurales:

Capacitación especializada continua de fiscales y jueces en evidencia digital.

Infraestructura tecnológica adecuada para análisis forense.

Protocolos claros de cadena de custodia electrónica.

Cooperación internacional inmediata y efectiva.

Interpretación restrictiva y garantista de los tipos penales.

Sin estos elementos, la respuesta penal corre el riesgo de oscilar entre ineficacia investigativa y sobre expansión punitiva.

La discusión revela que el reto no es meramente técnico, sino constitucional, el Estado debe equilibrar la necesidad de proteger la seguridad colectiva frente a organizaciones criminales altamente sofisticadas con la obligación de preservar los derechos fundamentales que constituyen la esencia del Estado de derecho, la expansión acrítica del derecho penal digital puede generar herramientas de vigilancia que, en contextos de debilidad institucional, resulten más peligrosas que el propio fenómeno que se intenta combatir.

La criminalidad organizada en entornos digitales exige una respuesta integral que combine fortalecimiento institucional, innovación tecnológica, cooperación transnacional y fidelidad estricta a los principios del garantismo penal, solo bajo este enfoque sistémico será

posible reducir la incidencia delictiva sin sacrificar la legitimidad democrática del sistema penal ecuatoriano.

CONCLUSIONES

La criminalidad organizada en entornos digitales se consolida como una de las expresiones más complejas de la macrocriminalidad contemporánea, al integrar estructuras jerarquizadas, dinámicas transnacionales y herramientas tecnológicas de alta sofisticación. En el contexto ecuatoriano, este fenómeno revela una tensión estructural entre la acelerada mutación de las formas delictivas y la capacidad real del sistema penal para investigarlas, procesarlas y sancionarlas dentro de los límites del Estado constitucional de derechos.

El estudio ha permitido constatar que, aunque el Código Orgánico Integral Penal incorpora figuras relativas a la delincuencia organizada y a los delitos informáticos, la eficacia normativa no depende exclusivamente de la tipificación formal, la brecha entre regulación y operatividad sigue siendo significativa. Las limitaciones en peritaje digital, la insuficiente especialización de operadores judiciales, las deficiencias en cadena de custodia electrónica y la complejidad probatoria en escenarios de automatización tecnológica dificultan la atribución rigurosa de responsabilidad penal, especialmente cuando intervienen estructuras descentralizadas o sistemas basados en inteligencia artificial.

La investigación evidencia que la expansión del poder punitivo frente a amenazas digitales no puede traducirse en una flexibilización de garantías fundamentales, la tentación de ampliar categorías penales o intensificar técnicas invasivas de investigación sin controles estrictos compromete principios esenciales como legalidad, proporcionalidad, presunción de inocencia y debido proceso. En consecuencia, el fortalecimiento de la respuesta penal debe articularse bajo un enfoque garantista, que asegure que la eficacia investigativa no se convierta en justificación para la erosión de derechos.

De igual manera, la dimensión transnacional del fenómeno exige superar enfoques estrictamente territoriales y avanzar hacia mecanismos de cooperación internacional más ágiles y coordinados, la criminalidad organizada digital no reconoce fronteras físicas por ello, su combate requiere interoperabilidad técnica, intercambio oportuno de información y armonización normativa regional.

La respuesta frente a la criminalidad organizada en el ciberespacio no puede reducirse a reformas legislativas aisladas, se requiere una estrategia estructural que integre fortalecimiento institucional, inversión sostenida en capacidades tecnológicas, formación especializada permanente, protocolos claros de manejo de evidencia digital y criterios dogmáticos precisos para la imputación en contextos de automatización y uso instrumental de inteligencia artificial.

Solo mediante un sistema penal técnicamente preparado, constitucionalmente limitado y estratégicamente coordinado será posible enfrentar con legitimidad y eficacia las nuevas formas

de criminalidad organizada, reducir los márgenes de impunidad y garantizar una protección real de los derechos fundamentales en la era digital.

REFERENCIAS

Acevedo Vásquez, D. P., Soto Palomino, Y., & Virhuez Cerna, F. E. (2022). Criminalidad organizada, lavado de activos y extinción de dominio en el Perú. Giuristi: Revista de Derecho Corporativo, 3(5), 78–93. https://doi.org/10.46631/Giuristi.2022.v3n5.06

Agra, F., & Silva, V. (2022). La digitalización del miedo: Del terrorismo "clásico" al terrorismo "tecnológico". El Criminalista Digital. Papeles de Criminología, (10), 17–37. https://produccioncientifica.ugr.es/documentos/643841e1cd47bb6af696c9fb

Agra, M. (2022). Terrorismo y ciberdelincuencia en el Código Penal español. Revista de Derecho Penal y Criminología. https://revista.cortesgenerales.es/rcg/article/download/473/1175/

Almenar Pineda, F. (2025). Las ultrafalsificaciones como delito en el anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales. Revista Ius Criminale, (2). https://doi.org/10.69592/3045-6681-N2-ABRIL-2025-ART-5

Asua Batarrita, A. (2006). El concepto jurídico-penal de terrorismo. Tirant lo Blanch.

Cabrera,(2025). Derecho penal y crimen organizado. Palestra Editores. https://dspace.udla.edu.ec/bitstream/33000/18529/1/UDLA-EC-TMDPCC-2025-15.pdf

Cancio Meliá, M. (2010). Los delitos de terrorismo: estructura típica y límites. Civitas. https://www.editorialreus.es/static/pdf/primeraspaginas_9788429015843_losdelitosdeterrorismo.pdf

Caraballo, J. (2020). El bien jurídico protegido en el delito de lavado de activos: análisis doctrinal contemporáneo. Revista de Derecho Penal y Criminología. https://revistas.uned.es/index.php/RDPC

Caraballo, P. G. (2020). Lavado de activos: Orígenes, situación actual y su problemática en entornos digitales. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3582257

Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus Protocolos (Protocolo de Palermo). (2000). Naciones Unidas. https://www.unodc.org/unodc/es/organized-crime/intro/UNTOC.html

Coxaj Caguay, L. (2024). La tecnología: Un detonante para la prevención y una nueva forma de enfrentar la criminalidad. Revista Diversidad Científica, 4(2), 105–113. https://doi.org/10.36314/diversidad.v4i2.132

Ferrajoli, L. (2006). Derecho y razón: Teoría del garantismo penal (10.ª ed.). Trotta. https://www.trotta.es/libros/derecho-y-razon/9788481641510/

Fuentes Tenorio, E. (2025). Criminalidad en el ciberespacio: Tipificación de delitos informáticos y desafíos probatorios en Ecuador. Polo del Conocimiento, 10(6), 2342–2350. https://doi.org/10.23857/pc.v10i6.9817

Gamón, A. (2017). Ciberdelincuencia y terrorismo digital. Editorial Jurídica. https://dialnet.unirioja.es/

Global Initiative Against Transnational Organized Crime. (2021). Global Organized Crime Index 2021. https://globalinitiative.net/analysis/ocindex-2021/

Global Initiative Against Transnational Organized Crime. (2023). Global Organized Crime Index 2023. https://globalinitiative.net/analysis/ocindex-2023/

Lagos Flores, R. (2024). Criminalidad organizada transnacional: De la seguridad pública a la amenaza geopolítica. Politai: Revista de Ciencia Política, 15(25), 17–32. https://doi.org/10.18800/politai.202402.001

Lamarca Pérez, C., & Mira Benavent, J. (2013). Derecho penal. Parte especial (3.ª ed.). Tirant lo Blanch. https://www.tirant.com/

López Calera, N. (2002). Terrorismo y derechos fundamentales. Tecnos. https://www.tecnos.es/

Montoya, Y. (2016). Manual sobre el delito de trata de personas. Instituto de Democracia y Derechos Humanos PUCP. https://idehpucp.pucp.edu.pe/

Morán Espinosa, A. (2021). Responsabilidad penal de la inteligencia artificial (IA): ¿La próxima frontera? Revista IUS, 15(48), 289–323. https://doi.org/10.35487/rius.v15i48.2021.706

Organización de las Naciones Unidas contra la Droga y el Delito (UNODC). (2022). Global Report on Trafficking in Persons 2022. https://www.unodc.org/unodc/en/data-and-analysis/glotip.html

Organización de las Naciones Unidas contra la Droga y el Delito (UNODC). (2024). Global Report on Organized Crime and Digitalization. https://www.unodc.org/

Reyes Valdivia, C. A. (2025). Tendencia de la criminalidad organizada en el Perú: Enfocada en la trata de personas. Revista de Ciencia e Investigación en Defensa, 6(1), 29–57. https://doi.org/10.58211/ty0bd952

Rosas, J. A., Percovich, A. E., & Colp, E. A. (2025). El uso del informe de inteligencia policial como prueba en procesos judiciales contra la criminalidad organizada. ESCPOGRAPNP, 4(2), 128–141. https://doi.org/10.59956/escpograpnpv4n2.9

Sampó, C. (2017). La diversidad del crimen organizado en América Latina: Una propuesta de clasificación. Revista de Relaciones Internacionales, Estrategia y Seguridad, 12(2), 195–219. https://doi.org/10.18359/ries.2218

Zaffaroni, E. R. (2015). La cuestión criminal. Planeta. https://www.planetadelibros.com/